IN THE CLAIMS:

All pending claims and their present status are produced below.

1.-29. (Cancelled)

30. (New) A computer-implemented method for use on a network to analyze a network resource from a remote location, comprising:

providing vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system, based on responses from the network resource satisfying conditions of the vulnerability detection rules; and

providing intrusion detection rules, corresponding to the selected vulnerabilities, for examining network traffic for attacks on the at least one of the determined application and the determined operating system responsive to the network traffic satisfying conditions of the intrusion detection rules.

31. (New) The method of claim 30, further comprising:

detecting the at least one of the application and the operating system,

wherein the intrusion detection rules are automatically provided upon detection.

32. (New) A method for use on a network to analyze a network resource from a remote location, comprising:

providing vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system, based on responses from the network resource satisfying conditions of the vulnerability detection rules.

33. (New) The method of claim 32, wherein the responses from the network resources comprise reflex signatures indicative of the at least one of the determined application and the determined operating system.

34. (New) The method of claim 32, further comprising:

prior to providing the vulnerability detection rules, generating templates to associate vulnerabilities with applications and operating systems,

wherein a vulnerability detection rule selecting vulnerabilities selects a template corresponding to the determined application or the determined operating system.

35. (New) The method of claim 34, wherein a vulnerability detection rule comprises a complex rule that establishes logical relationships between two or more templates, and

wherein a vulnerability detection rule selecting vulnerabilities selects the two or more templates.

36. (New) The method of claim 32, further comprising:

providing vulnerability detection rules for detecting the network resource on the network, and for selecting vulnerabilities associated with network resources having any operating system.

37. (New) The method of claim 32, further comprising:

providing vulnerability detection rules for detecting a specific open port on the network resource, and for selecting vulnerabilities associated with the specific open port.

38. (New) The method of claim 32, wherein a vulnerability detection rule determining at least one of the determined application and the determined operating system on the network resource comprises a challenge-response test to send data to the network resource and elicit a response indicative of the a least one of the determined application and the determined operating system.

39. (New) The method of claim 32, wherein the determined application comprises one or more from the group containing: tcmmux, echo, netstat, ftp, telnet and a network service.

40. (New) The method of claim 32, further comprising:

providing intrusion detection rules for examining network traffic responsive to the selected vulnerabilities.

41. (New) The method of claim 40, wherein intrusion detection rules for examining network traffic examine one or more fields of a network packet for predetermined values indicative of the selected vulnerabilities.

42. (New) The method of claim 40, wherein intrusion detection rules detects an attack on the selected vulnerabilities responsive the network traffic satisfying conditions of the intrusion detection rules.

43. (New) A device for use on a network to analyze a network resource from a remote location, comprising:

a database to store vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system, based on responses from the network resource satisfying conditions of the vulnerability detection rules,

the database also configured to store intrusion detection rules for examining network traffic for attacks on at the least one of the determined application and the determined operating system responsive to the selected vulnerabilities, based on the network traffic satisfying conditions of the intrusion detection rules.

44. (New) The device of claim 43, further comprising:

a vulnerability detection system to determine the at least one of the application and the operating system and select the vulnerabilities using the vulnerability detection rules; and

an intrusion detection system, in communication with the vulnerability detection system, to automatically examine the netowk responsive to the selected vulnerabilities.

45. (New) A device for use on a network to analyze a network resource from a remote location, comprising:

a database to store vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system, based on responses from the network resource satisfying conditions of the vulnerability detection rules.

46. (New) The device of claim 45, wherein the responses from the network resources comprise reflex signatures indicative of the at least one of the determined application and the determined operating system.

47. (New) The device of claim 45, further comprising:

a graphical user interface to provide a template for associating vulnerabilities with applications and operating systems,

wherein a vulnerability detection rule selecting vulnerabilities selects a template.

48. (New) The device of claim 47, wherein a vulnerability detection rule comprises a complex rule that establishes logical relationships between two or more templates, and

wherein a vulnerability detection rule selecting vulnerabilities selects the two or more templates.

49. (New) The device of claim 45, wherein the database stores vulnerability detection rules for detecting the network resource on the network, and for selecting vulnerabilities associated with any network resources having an operating system.

50. (New) The device of claim 45, wherein the database stores vulnerability detection rules for detecting a specific open port on the network resource, and for selecting vulnerabilities associated with the specific open port.

51. (New) The device of claim 45, wherein a vulnerability detection rule determining at least one of the determined application and the determined operating system on the network resource comprises a challenge-response test to send data to the network resource and elicit a response indicative of the at least one of the determined application and the determined operating system.

52. (New) The device of claim 45, wherein the determined application comprises one or more from the group containing: tcmmux, echo, netstat, ftp, telnet and a network service.

53. (New) The device of claim 45, wherein the database also stores intrusion detection rules for examining network traffic responsive to the selected vulnerabilities.

54. (New) The device of claim 53, wherein intrusion detection rules for examining network traffic examine one or more fields of a network packet for predetermined values indicative of the selected vulnerabilities.

55. (New) The device of claim 53, wherein intrusion detection rules detects an attack on the selected vulnerabilities responsive the network traffic satisfying conditions of the intrusion detection rules